AMENDMENTS TO THE SPECIFICATION

In the Specification:

Please amend paragraph three as shown.

However, there are drawbacks to both cases. Email systems have severe restrictions on transferring files (*e.g.*, size, type of files, and issues with security and privacy). The server solution is not available to a majority of users in a secure way, since subscribers of, for example, a DSL (Digital Subscriber Line) service would be placing the server machine outside of the local gateway/firewall, and to some extent, exposing the shared files. This solution is not feasible in many scenarios, however, due to storage size restrictions, security concerns, costs, etc. Even when considered "secure", the provider cannot totally guarantee data security, since new security holes are discovered ~~on~~ periodically in products. For at least this reason, a majority of users are skeptical of placing confidential information and critical files on publicly-accessible servers or networks.

Please amend paragraph four as shown.

Moreover, in order to share data between computers that are separated by firewalls (and on different networks) the user typically must go through a laborious exercise that requires much more than a basic understanding of interacting with a computer. A technical knowledge is required that is beyond the knowledge of the average user to configure the user's computer to perform data sharing behind firewalls. Even if configured correctly, newly discovered security holes can enable unauthorized access by hackers to secure information. The user must understand the technologies involved, as well as applications suitable for specific data sharing scenarios. Thus, placing a computer on an open network (*e.g.*, the Internet) requires continuous maintenance to ensure that security holes are plugged.

Please amend paragraph twenty-six as shown.

An authorization component 118 verifies if the request 106 is associated with the private key 120 and ~~that~~ permits access to the file 112. If so, a communications component 122 establishes a secure tunnel 124 to the requestor 108 of the request 106. The communications component 122 only permits access to the particular data 112, and the data 112 passing through the tunnel 124 is encrypted. The system 100 further includes a permissions component 126 that determines levels of access permitted or assigned to entities outside the firewall 116. The communications component 122 only permits access to the particular data 112. There can be a total access level, and a plurality of limited access levels, *e.g.*, read-only, and modification (overwriting access). Moreover, the communications component 122 only permits uni-directional flow of the data 112 after the request 106 is passed through to the sharor 114. This prevents the spread of computer viruses and other unfiltered attacks.

Please amend paragraph fifty-one as shown.

Referring now to FIG. 5, there is a system 500 that illustrates a capability of the present invention for a requestor ~~502~~ to obtain data in accordance with differing levels of permissions and a data class. These deferring levels can be facilitated in the user computer operating system or other supporting application by allowing the user to select the data, and then right-click to edit the properties associated therewith such that the data includes attributes associated with a class of data, a certain request, and modification permissions, for example. A sharor 502 (similar to sharors 114) registers with a service 504. In response, the service 504 generates one or more keys 506 associated with each or a plurality of the data (508, 510, and 512) intended for sharing. When the requestor 108 sends a request to the service 504, the service 504 extracts the share data therefrom to retrieve the appropriate keys 506. If there is only one key required to return the requested data, the service 504 extends a secure tunnel to the requestor 108 (the tunnel already in existence between the sharor 502 and the service 504 due to any one of the keys generated by the service 504). If there is more than one request submitted to the service 504, a separate tunnel for each request can be opened from the sharor 502 to the requestor

in a consecutive or concurrent manner. Alternatively, the service 504 is sufficiently sophisticated to process bundles of requests from a single requestor to a single sharor, and maintain a single tunnel for the multiple requests to the same sharor 502.

Please amend paragraph sixty-one as shown.

The first proxy server 706 further includes a plurality of proxy services 714, 716, and 718 (also denoted respectively as $SERVICE_1$, $SERVICE_2$, and $SERVICE_3$). Thus, within the first proxy server 706, a second classifier 720 is employed to selectively utilize one or more of the resident services 714, 716, and 718, based upon loading balancing parameters processed by the classifier 720. Both the system classifier 712 and server classifier 720 operate according to the classifier description provided hereinabove. The system classifier 712 interfaces to the first proxy server classifier 720 to facilitate load balancing between the resident services 714, 716, and 718, and the system proxy servers 706, 708, and 710. The first proxy server 706 also includes a key repository 722 that stores keys generated by at least the sharor 114 registering data for sharing. Of course, the remaining proxy servers 708 and 710 can have the same or similar capabilities of the first server 706.

Please amend paragraph sixty-seven as shown.

Alternatively, the client software, with the aid of the classifier, can automatically estimate the level of security of the local sharor environment, and impose that same level on the requestor through the accompanying rule file. Thus, a data that has now been received by requestor, can be opened only with a fully authorized client that has the key. If the client is unauthorized or is an uncertified copy, then the user either is totally prohibited from viewing the data or can be allowed a limited view, *e.g.*, header data or short summary of data, but not all of the data.

Please amend paragraph sixty-eight as shown.

In another implementation, the sharor and requestor are not based on a unique location ID, but a user ID. That is, the tunnel is created based upon a sharor user ID and a requestor user ID, in a person-to-person connection. Thus, data sharing is not restricted to a particular machine or device. This facilitates the utilization of any computing devices capable of wired or wireless communication (*e.g.*, a PDA or portable telephone with such capabilities) for data sharing between the persons. The request then includes a personal ID of the requesting person. The shared data can be uploaded to a storage location associated with the personal ID, which storage location can be anywhere on the network, including the current computing device the person is using. The input of the personal ID causes the request to ~~sent~~ send, either by the computing device client or by a third party service, for example. Authentication of the person would not necessarily be required; however, it could also be implemented as an additional security measure.